ASSISTANT TO THE SECRETARY OF DEFENSE
1400 DEFENSE PENTAGON
WASHINGTON, DC
20301-1400

PUBLIC AFFAIRS

APR 29 2016

MEMORANDUM FOR MILITARY SERVICE PUBLIC AFFAIRS CHIEFS

SUBJECT: Department of Defense Public Affairs Guidance for Official Use of Social Media

Social media is a powerful tool for communicating with the public and collaborating within the Department, as well as providing service members access to their loved ones even when they are stationed thousands of miles away. Pentagon officials at the highest levels recognize the importance of including social media as part of a comprehensive public affairs strategy, consistent with DoD Instruction 5400.14, "Procedures for Joint Public Affairs Operations," November 3, 2014. The Department's overarching policies for its use are provided in DoD Instruction 8550.01, "DoD Internet Services and Internet-Based Capabilities," September 11, 2012.

The attached document outlines OSD guidance and best practices for use by social media practitioners and PA staff who oversee and maintain official DoD accounts.

Social media technologies should be used to enhance communication, collaboration, and information exchange in support of our mission. It is important to remember that social media changes over time: strategies that work today may be less effective tomorrow. If we rely only on existing media strategies for information dissemination, we may miss important opportunities.

The information in the attached document does not supersede or replace existing legal authorities and policies in effect, but is intended to provide supplemental guidance specific to social media use. While this guidance is primarily directed toward official DoD uses of social media, Department personnel remain bound by the Standards of Ethical Conduct for Employees of the Executive Branch and the Hatch Act regardless of the social media platform or whether DoD systems are used. In general, the use of social media technology follows the same standards of professional practice and conduct associated with everything else we do, and exercising common sense and sound judgment in the use of social media will help users avoid various problematic scenarios.

If you have any questions about this guidance, please contact Stephanie Dreyer in OATSD(PA), stephanie.l.dreyer.civ@mail.mil.

Peter C. Cook

Peter C. Cook
Acting

Attachment:
As stated

Department of Defense Public Affairs Guidance for Official Use of Social Media

References: (a) DoD Instruction 8550.01, “DoD Internet Services and Internet-Based Capabilities,” September 11, 2012
(b) DoD Directive 5535.09, “DoD Branding and Trademark Licensing Program,” December 19, 2007
(c) DoD Instruction 5015.02, “DoD Records Management Program,” February 24, 2015
(d) DoD Administrative Instruction 15, “OSD Records and Information Management Program,” May 3, 2013
(e) Office of Government Ethics’ (OGE) Legal Advisory, LA-15-03, “The Standards of Conduct as Applied to Personal Social Media Use,” April 9, 2015
(f) DoD 5500.7-R, “Joint Ethics Regulation (JER),” August 30 1993

This attachment contains OSD guidance and best practices for use by social media practitioners and PA staff who oversee and maintain official DoD accounts (e.g. a Uniformed Service’s official Twitter page). The implementation of this guidance is effective immediately.

Social media platforms, technology and uses are dynamic and the ability to adapt to changing trends and technologies to will be imperative in order to take full advantage of social media as a communication tool and as part of a comprehensive strategy for the Department of Defense.

Guidance:

I. Establishing an Initial Presence:

A. Approval for official accounts (e.g. External Official Presence (EOP))

EOP activities should be conducted in compliance with the general requirements listed in DoD Instruction 8550.01 (Reference (a)). Before establishing an EOP, approval should be obtained from the responsible DoD Component Head.

Procedures for applying for an official social media account are provided in Enclosure 3 of DoD Instruction 8550.01 (Reference (a)).

It is recommended that only accounts with a dedicated Public Affairs Office (PAO) and a written strategy plan should apply for official verification (the “blue check mark”) from specific social media sites. Applicants should submit verification requests to the Digital Engagement Lead for each Uniformed Service or combatant command in coordination with the OATSD(PA) Director of Digital Media.

B. Negotiated Terms of Service agreements

Before deciding to use a social media tool (e.g. Facebook, Instagram), one should seek the advice of the appropriate agency Terms of Service (TOS) Point of Contact (POC) to be sure the agency has already signed a federal-compatible TOS, that the product supports broader agency mission and goals, and that the TOS is legally appropriate for use by that agency. See complete implementation guidance on the main Terms of Service page.

C. Registering an account

All DoD owned and operated social media accounts should be registered at http://www.defense.gov/Sites/Register-A-Site and are encouraged to register with the U.S. Digital Registry at https://www.digitalgov.gov/services/u-s-digital-registry/. When possible, consider registering with an email address linked to the organization overseeing the account and not a specific person so that the email remains valid through personnel changes. Registrations in these sites make it possible to confirm the validity of a variety of government social media accounts.

II. Maintaining an Official Presence:

A. Clearly identify DoD affiliation

In maintaining an official presence, components should adhere to the following:

- Clear identification that a DoD component is supplying the content for the EOP should be provided.

- The DoD Component under which the EOP is managed, the mission of that Component, and the purpose of the EOP should be provided, as workable.

- Official branding should be in accordance with DoD Directive 5535.09 (Reference (b)).

B. Appropriate content

Although social media is more informal and conversational than conventional military communications, PA staff using social media must remain professional at all times and remember that each platform is simply another tool to achieve the DoD mission. The following are some examples to use as guidelines:

- Do not post graphic, obscene, explicit or racial comments, or comments that are abusive, hateful, vindictive or intended to defame anyone or any organization.

- As a general rule, do not post promotional material or advertisements for a non-federal entity, including its products, services, or sponsored events. Certain exceptions may apply, however, so consult with the appropriate ethics official.

- Do not post details about an ongoing investigation, legal or administrative proceeding that could prejudice the processes or interfere with an individual's rights.

- Avoid spamming or trolling which may be removed and may cause the author(s) to be blocked from the page without notice.

- Do not post copyrighted or trademarked content without permission of the copyright or trademark owner. Imagery posted on social media should be owned by the user. It is acceptable to link to trademarked content if an appropriate citation is provided.

- Be careful to not post comments, photos or videos that suggest or encourage illegal activity.

- Avoid politically oriented content. For additional guidance, see: https://osc.gov/Resources/FAQ%20Hatch%20Act%20Employees%20and%20Social%20Media%20Nov%202015.pdf

All information posted to social media sites should be unclassified. In addition information that is For Official Use Only (FOUO), pre-decisional, proprietary, business-sensitive, or protected by the Privacy Act should not be posted without explicit authorization. Ensure that posted information is marked appropriately, as necessary. Do not post personnel lists, rosters, or directories.

- Remember that use of a government or commercial social media site in an official capacity (related to organizational mission) constitutes official communication. Accuracy and propriety are imperative.

III. Additional Best Practices:

A. Handling social media mistakes

Extensive use of social media may result in occasional mistakes. Follow these steps in the event of a posting error or other mistake:

- Maintain all efforts to remain transparent; delete or edit the post and apologize for the mistake as appropriate, and explain that the material was posted in error and is not an official view.

- If the mistake was factual, post the factually correct information, making clear what has been clarified.

- Refer to the individual digital leads in the appropriate Uniformed Service or DoD component for further guidance.

B. Keeping social media sites safe

Social media access and content need to be defended and protected with vigilance. Cyber-attacks are a real and present threat to the security of government social media accounts. Below are some best practices for keeping social media sites safe:

- Use a strong password. At least 20 characters long, that is either randomly-generated (like LauH6maicaza1Neez3zi) or a random string of words (like "hewn cloths titles yachts refine"). Use a unique password for each website or service to ensure that if one account gets compromised the rest remain safe.

- Use a government e-mail address for official accounts, also with a strong password. A .mil or .gov account will generally be more secure than a personal account, and will reduce the possibility of unauthorized password-reset and interception of emails. Consider added precautions such as two-factor authentication.

- Do not give untrusted third parties, including those who promise more followers or financial returns, access to account usernames and passwords.

- Select third-party applications with care. There are thousands of applications built by external developers that allow an array of innovative functions with an account. Control of a government social media site account should not be given to anyone outside of the command or organization. Revoke access for any third-party application that is not recognized by visiting the Applications tab in the platform's account settings.

- Make sure all computers and operating systems are up-to-date with the most recent patches, upgrades, and anti-virus software, and that all computers and mobile devices are protected by secure passwords.

- Change social media account passwords at a regularly scheduled time (e.g. once a quarter). Never send passwords via email, even internally.

- **Use extra security features** to help keep accounts protected. For example, Facebook has such instructions here.

- **Minimize the number of people who have access to the account.** Even if a third-party platform is used to avoid sharing the actual account passwords, each person is a possible avenue for phishing or other compromise.

- Report all security violations (e.g. hacked accounts, impostors, etc.) through the appropriate DoD security channels and the Digital Engagement Leads, as well as appropriate social media provider channels (e.g. online forms). For example, to report a violation on Twitter, in addition to reporting through DoD channels, file a security ticket at https://support.twitter.com/forms/.

C. Making use of social media analytics (tracking and reporting)

The majority of social platforms offer more data, either through third party tools or internal "analytics," than has typically been available to PA practitioners. For example, Facebook offers analytics in their "insights page" and Twitter has an "analytics" page. This information is best used for two key purposes: guiding strategy and reporting impact.

Strategy

- Social platforms and audience methods of consumption change so rapidly that current effective posting strategies may become ineffective in a short period of time. Social media practitioners need to have an adaptable strategy. The best way to inform that strategy is to use the analytical tools available on each platform or seek a third party tool (e.g. Hootsuite, sprout social, Radian6).

- Evaluate the intended audience. Review the data to track current followers, as well as whom the content reaches and who engages with it.

- Find patterns in successful posts. Analyze which posts achieve the best results and why. However, this step will become ineffective if posts are constructed the same way each time, so do not be afraid to test different tactics:
    - Experiment (develop a different type of post/campaign/presentation)
    - Engage (reply to a comment or create calls to action)
    - Measure (analyze impact)
    - Repeat (alter the post as necessary as informed by measurement).

Reporting

- While far from perfect, it is possible to measure the impact of one's communication efforts more than ever before. As communications professionals, it is important to provide easily understood, clearly focused reports to commanders.

- Be the translator. For example, explain what a "like" and an "engagement" are. Reports need to be clearly understood by non-social media practitioners. Be sure to provide context to reports.

- Focus on what is important. Avoid providing numbers for the sake of numbers. Reporting should be done when there is a measurable impact on a required objective, or actionable data can be provided to the commander. Reach, impressions, and engagements may have meaning to social media managers, but not to commanders.

- Be clear about what metrics will be prioritized and why. As an example, some organizations may prefer to focus on the number of "likes" as a measure of success. Others will choose to focus on shares.

D. Personal use of social media

For personal social media accounts, the user need not include DoD affiliation in a profile. Remember that even when posting in a personal capacity, others may still identify a poster's

DoD affiliation, even if not included in the public profile. Stating that one's views are personal does not remove the risk of negative media or other publicity. Social media practitioners should always keep in mind that posts can be shared outside of one's personal network.

Please follow Executive Branch-wide guidance for personal social media usage during work hours (*see Office of Government Ethics' (OGE) Legal Advisory, LA-15-03: The Standards of Conduct as Applied to Personal Social Media Use*, https://www.oge.gov/web/oge.nsf/Legal%20Advisories/16D5B5EB7E5DE11A85257E96005FBF13/$FILE/LA-15-03-2.pdf?open Reference (e)), in addition to pertinent guidance in DoD Instruction 8550.01 (Reference (a)) and the Joint Ethics Regulation (Reference (f)).

IV. **Records Management:**

DoD components should create an internal records management process and should work with their service component electronic records management office to establish this process, in accordance with DoD Instruction 5015.02 (Reference (c)) and DoD Administrative Instruction 15 (Reference (d)).